LINKSYS®

A Division of Cisco Systems, Inc.

2.4GHz 802.11g

Wireless-G

Access Point with Power Over Ethernet

User Guide

WIRELESS

Model No. **WAP54GP**

CISCO SYSTEMS

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2005 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

WARNING: This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

How to Use this User Guide

The user guide to the Wireless-G Access Point with Power Over Ethernet has been designed to make understanding networking with the Access Point easier than ever. Look for the following items when reading this User Guide:

This checkmark means there is a note of interest and is something you should pay special attention to while using the Access Point.

This exclamation point means there is a caution or warning and is something that could damage your property or the Access Point.

This question mark provides you with a reminder about something you might need to do while using the Access Point.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: *definition.*

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the “List of Figures” section.

Table of Contents

Chapter 1: Introduction 1
Welcome 1
What's in this User Guide? 2
Chapter 2: Planning Your Wireless Network 4
Network Topology 4
Roaming 4
Network Layout 5
Chapter 3: Getting to Know the Wireless-G Access Point with Power Over Ethernet 6
The Front Panel 6
The Back Panel 7
Chapter 4: Connecting the Wireless-G Access Point with Power Over Ethernet 8
Overview 8
Connections for Setup 8
Placement Options 9
Chapter 5: Setting Up the Wireless-G Access Point 10
Overview 10
Accessing the Utility 10
Navigating the Utility 11
Chapter 6: Configuring the Wireless-G Access Point 13
The Setup Tab 13
The Setup - Time Tab 14
The Wireless - Basic Wireless Settings Tab 15
The Wireless - Wireless Security Tab 17
The Wireless - Wireless Connection Control Tab 22
The Wireless - Advanced Wireless Settings Tab 23
The AP Mode Tab 25
The Administration - Management Tab 28
The Administration - Log Tab 30
The Administration - Factory Default Tab 32
The Administration - Firmware Upgrade Tab 32
The Administration - Reboot Tab 33
The Administration - Config Management Tab 34

The Status - Local Network Tab 35
The Status - Wireless Tab 36
The Status - System Performance Tab 37
Appendix A: Troubleshooting 39
Frequently Asked Questions 39
Appendix B: Wireless Security 43
Security Precautions 43
Security Threats Facing Wireless Networks 43
Appendix C: Upgrading Firmware 46
Appendix D: Windows Help 47
Appendix E: Glossary 48
Appendix F: Specifications 53
Appendix G: Warranty Information 55
Appendix H: Regulatory Information 56
Appendix I: Contact Information 62

List of Figures

Figure 3-1: Front Panel 6
Figure 3-2: Back Panel 7
Figure 4-1: Connect the Ethernet Network Cable 8
Figure 4-2: Connect the Power 8
Figure 4-3: The Access Point's Stand Slots 9
Figure 4-4: The Access Point's Wall-Mount Slots 9
Figure 5-1: Login Screen 10
Figure 6-1: Setup - Static IP Address 13
Figure 6-2: Setup - Automatic Configuration - DHCP 14
Figure 6-3: Setup - Time 14
Figure 6-4: Wireless - Basic Wireless Settings 15
Figure 6-5: Wireless - Wireless Security (Disabled) 17
Figure 6-6: Wireless - Wireless Security (WPA-Personal) 17
Figure 6-7: Wireless - Wireless Security (WPA2-Personal) 18
Figure 6-8: Wireless - Wireless Security (WPA2-Personal Mixed) 18
Figure 6-9: Wireless - Wireless Security (WPA-Enterprise) 19
Figure 6-10: Wireless - Wireless Security (WPA2-Enterprise) 19
Figure 6-11: Wireless - Wireless Security (WPA2 - Enterprise Mixed) 20
Figure 6-12: Wireless Security - RADIUS 21
Figure 6-13: Wireless Settings - WEP 21
Figure 6-14: Wireless - Wireless Connection Control 22
Figure 6-1: Select MAC Address from Client Association Table 22
Figure 6-15: Wireless - Advanced Wireless 23
Figure 6-16: AP Mode 25
Figure 6-17: Wireless Repeater 26
Figure 6-18: Site Survey 27
Figure 6-19: Administration - Management 28
Figure 6-20: The Administration - Log 30

Figure 6-21: Administration - Factory Default 32
Figure 6-22: Administration - Firmware Upgrade 32
Figure 6-23: Administration - Reboot 33
Figure 6-24: Administration - Config Management 34
Figure 6-25: Status - Local Network 35
Figure 6-26: Status - Wireless 36
Figure 6-27: Status - System Performance 37
Figure C-1: Firmware Upgrade 46

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Access Point with Power Over Ethernet. This Access Point will allow you to network wirelessly better than ever.

How does the Access Point do all of this? An access point allows for greater range and mobility within your wireless network while also allowing you to connect the wireless network to a wired environment. In fact, the Wireless-G Access Point with Power Over Ethernet can support communications on up to eight wireless networks, using Virtual Local Area Network (VLAN) technology.

The Wireless-G Access Point with Power Over Ethernet also offers the convenience of Power over Ethernet (PoE) capability, so it can receive data and power over a single Ethernet network cable.

But what does all of this mean?

Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun.

PCs on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called "wired".

PCs equipped with wireless cards and adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network. This is sometimes called a WLAN, or Wired Local Area Network. The Access Point bridges wireless networks of both 802.11g and 802.11b standards and wired networks.

Use the instructions in this Guide to help you connect the Access Point, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the Access Point.

***access point**: a device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.*

***network:** a series of computers or devices connected together.*

***lan** (local area network): the computers and networking products that make up your local network.*

***poe** (power over ethernet): a technology enabling an Ethernet network cable to deliver both data and power.*

***ethernet:** network protocol that specifies how data is placed on and retrieved from a common transmission medium.*

***adapter:** a device that adds network functionality to your PC.*

***802.11g:** a wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.*

***802.11b:** a wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.*

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G Access Point with Power Over Ethernet.

- Chapter 1: Introduction
  This chapter describes the Access Point's applications and this User Guide.
- Chapter 2: Planning your Wireless Network
  This chapter describes the basics of wireless networking.
- Chapter 3: Getting to Know the Wireless-G Access Point with Power Over Ethernet
  This chapter describes the physical features of the Access Point.
- Chapter 4: Connecting the Wireless-G Access Point with Power Over Ethernet
  This chapter instructs you on how to connect the Access Point to your network.
- Chapter 5: Setting up the Wireless-G Access Point with Power Over Ethernet
  This chapter explains how to perform basic setting changes through the Web-based Utility.
- Chapter 6: Configuring the Wireless-G Access Point with Power Over Ethernet
  This chapter explains how to use the Access Point's Web-based Utility for advanced configuration.
- Appendix A: Troubleshooting
  This appendix describes some frequently asked questions regarding installation and use of the Access Point.
- Appendix B: Wireless Security
  This appendix explains the risks of wireless networking and some solutions to reduce the risks.
- Appendix C: Upgrading Firmware
  This appendix instructs you on how to upgrade the Access Point's firmware.
- Appendix D: Windows Help
  This appendix describes some of the ways Windows can help you with wireless networking.
- Appendix E: Glossary
  This appendix gives a brief glossary of terms frequently used in networking.
- Appendix F: Specifications
  This appendix provides the Access Point's technical specifications.
- Appendix G: Warranty Information
  This appendix supplies the Access Point's warranty information.

- Appendix H: Regulatory Information
  This appendix supplies the Access Point's regulatory information.

- Appendix I: Contact Information
  This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with one another to form an ad-hoc network.

***ad-hoc**: a group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.*

Linksys wireless adapters also provide users access to a wired network when using an access point, such as the Wireless-G Access Point with Power Over Ethernet, or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router.

***infrastructure**: a wireless network that is bridged to a wired network via an access point.*

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and may double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, providing that they both share the same channel and SSID.

***roaming**: the ability to take a wireless device from one access point's range to another without losing the connection.*

Before using the roaming capabilities, choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

***ssid**: your wireless network's name*

Network Layout

The Wireless-G Access Point with Power Over Ethernet has been designed for use with 802.11g and 802.11b products. The Access Point is compatible with 802.11g and 802.11b adapters, such as the Notebook Adapters for your laptop computers, PCI Adapters for your desktop PCs, and USB Adapters for when you want to enjoy USB connectivity. These wireless products can also communicate with a 802.11g or 802.11b Wireless PrintServer.

To link your wired network with your wireless network, connect the Access Point's Ethernet network port to any switch or router. If you want to use Power Over Ethernet (POE), then connect the Access Point to any switch or router that complies with the POE standard (802.3af)—or you can use a POE injector, such as the Linksys WAPPOE or WAPPOE12.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at *www.linksys.com* for more information about wireless products.

Chapter 3: Getting to Know the Wireless-G Access Point with Power Over Ethernet

The Front Panel

The Access Point's LEDs, which indicate activity and status information, are located on the front panel.

Power Green. The **Power** LED lights up when the Access Point is powered on.

Ethernet Green. The **Ethernet** LED lights up when the Access Point is successfully connected to a device through the Ethernet network port. If the LED is flashing, the Access Point is actively sending to or receiving data from one of the devices over the Ethernet network port.

Wireless-G Green. The **Wireless-G** LED lights up when the Access Point is successfully connected to a wireless device. If the wireless LED is flashing, the Access Point is actively sending to or receiving data from a wireless device.

Figure 3-1: Front Panel

The Back Panel

The Access Point's Ethernet network and power ports, as well as the Reset button, are located on the back panel.

Ethernet Port The Ethernet network port connects to an Ethernet network device, such as a switch or router.

Reset Button There are two ways to Reset the Access Point's factory defaults. Either press the **Reset** button, for approximately ten seconds, or restore the defaults using the Access Point's Web-based Utility.

IMPORTANT: Resetting the Access Point will erase all of your settings (including wireless security, IP address, and power output) and replace them with the factory defaults. Do not reset the Access Point if you want to retain these settings.

Power Port The Power port connects to the Access Point's power adapter. (This port will not be used if you are using Power Over Ethernet.)

port: *the connection point on a computer or networking device used for plugging in cables or adapters*

Figure 3-2: Back Panel

Chapter 4: Connecting the Wireless-G Access Point with Power Over Ethernet

Overview

This chapter explains how to connect the Access Point for setups.

Connections for Setup

1. Attach the Access Point's antenna.
2. Connect your Ethernet network cable to your network router or switch. Then connect the other end of the network cable to the Access Point's Ethernet port.
3. If you are using Power Over Ethernet (POE), proceed to the following section, "Placement Options."

   If you are not using POE, then connect the included power adapter to the Access Point's Power port. Then plug the power adapter into an electrical outlet. The LEDs on the front panel will light up as soon as the Access Point's powers on.

Proceed to the following section, "Placement Options."

Figure 4-1: Connect the Ethernet Network Cable

Figure 4-2: Connect the Power

NOTE: The Bridge features Power Over Ethernet (POE) support. POE technology allows a POE adapter (also known as a power injector, power hub, or inline power device) to supply data and power to an Ethernet device using a single Ethernet network cable. To use the Bridge's POE feature, follow the instructions for your specific POE device.

Placement Options

There are three ways to place the Access Point. The first way is to place it horizontally on a surface, so it sits on its four rubber feet. The second way is to stand the Access Point vertically on a surface. The third way is to mount it on a wall. The stand and wall-mount options are explained in further detail below.

Stand Option

1. Near the Access Point's bottom panel are two rubber feet and two rubber inserts. Remove them to expose the stand slots you want to use.
2. The Access Point includes four triangular stands. With its rubber pad facing the bottom, insert a stand into a slot, and push the stand upward until the stand snaps into place.

   Repeat this step with the other stands.

Now that the hardware installation is complete, proceed to "Chapter 5: Setting Up the Wireless-G Access Point with Power Over Ethernet," for directions on how to configure the Access Point.

Figure 4-3: The Access Point's Stand Slots

Wall-Mount Option

1. On one of the Access Point's side panels are four rubber feet. Remove four adjacent feet to expose the wall-mount slots you want to use. The distance between two adjacent slots is 145 mm (5.7 inches).
2. Determine where you want to mount the Access Point.
3. Drill four holes into the wall. Make sure adjacent holes are 145 mm (5.7 inches) apart.
4. Insert a screw into each hole, and leave 5 mm (0.2 inches) of its head exposed.
5. Maneuver the Router so the wall-mount slots line up with the four screws.
6. Place the wall-mount slots over the screws and slide the Access Point down until the screws fit snugly into the wall-mount slots.

Now that the hardware installation is complete, proceed to "Chapter 5: Setting Up the Wireless-G Access Point with Power Over Ethernet," for directions on how to configure the Access Point.

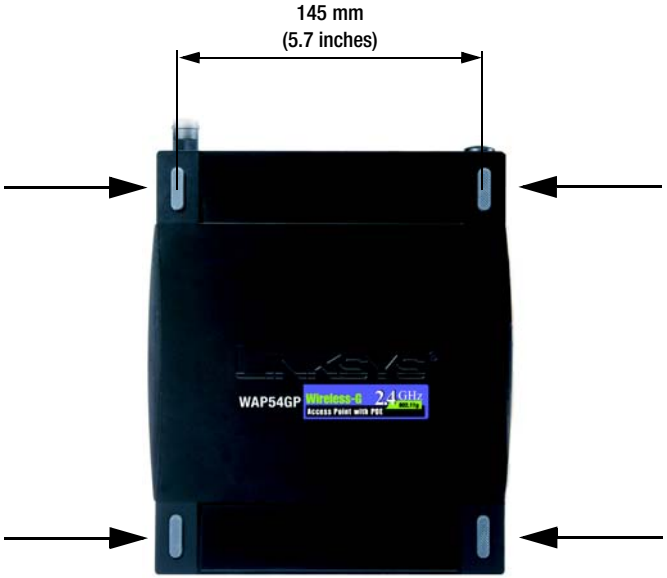


Figure 4-4: The Access Point's Wall-Mount Slots

Chapter 5: Setting Up the Wireless-G Access Point with Power Over Ethernet

Overview

The Access Point has been designed to be functional right out of the box with the default settings. However, if you'd like to change these settings, the Access Point can be configured through your web browser with the Web-based Utility. This chapter explains how to use the Utility.

The Utility can be accessed via web browsers, such as Microsoft Internet Explorer or Mozilla Firefox through the use of a computer that is networked with the Access Point.

For a basic network setup, most users only have to use the following screens of the Utility:

- Setup
  On the *Setup* screen, enter your basic network settings (IP address) here.

- Management
  Click the **Administration** tab and then select the **Management** screen. The Access Point's default password is **admin**. To secure the Access Point, change the AP Password from its default.

Most users will also customize their wireless settings:

- Wireless
  On the *Wireless* screen, change the default SSID under the **Basic Wireless Settings** Tab. Select the level of security under the **Wireless Security** Tab.

HAVE YOU: Enabled TCP/IP on your PCs? PCs communicate over the network with this protocol. Refer to "Appendix D: Windows Help" for more information on TCP/IP.

tcp/ip: *a set of protocols PCs use to communicate over a network.*

browser: *an application that provides a way to look at and interact with all the information on the World Wide Web.*

Accessing the Utility

There are three ways to connect to your Access Point for the first time.

1. If you have a 48V Power Injector (e.g. Linksys WAPPOE), power up your Access Point first, then connect the cable from your Injector to your PC. Configure your PC to have the static IP address on the same subnet as the Access Point's default IP address (192.168.1.245).

2. If you have a PoE switch (e.g. Linksys SRW224P), connect your Access Point and your PC to the same LAN. Configure your PC to have the static IP address on the same subnet as the Access Point's default IP address

Figure 5-1: Login Screen

(192.168.1.245). Or if there is DHCP server connected to the switch, configure it to assign the IP address in the192.168.1.0/24 subnet. Your PC will get an IP address in the subnet through the DHCP.

3. Although not recommended, you can connect your PC wirelessly to the Access Point when the DHCP server is connected on the LAN side. It is not recommended, because you can easily lose your connection through configuration changes.

Launch your web browser, such as Internet Explorer or Mozilla Firefox and enter the Access Point's default IP address, **192.168.1.245**, in the *Address* field. Press the **Enter** key.

Enter **admin** in the *User Name* field. The first time you open the Web-based Utility, use the default password, **admin**. (You can set a new password from the Administration - Management tab.) Then click the **OK** button.

After setting up the Access Point to use DHCP or manually configure a new IP address, move your Access Point to the desired network. You will have to use the new IP address the next time you access the Web-based Utility.

Navigating the Utility

The Web-based Utility consists of the following five main tabs: Setup, Wireless, AP Mode, Administration, and Status. Additional screens (sub tabs) will be available from most of the main tabs.

The following briefly describes the main & sub tabs of the Utility.

Setup

Enter the Host Name and IP Address settings on this screen.

Wireless

You will use the Wireless tabs to enter a variety of wireless settings for the Access Point.

- *Basic Wireless Settings*. Choose the wireless network mode (e.g. wireless-G), Virtual Local Area Network (VLAN) settings, SSIDs, and transmit rates on this screen.
- *Wireless Security*. Use this screen to configure the Access Point's security settings.
- *Wireless Network Access*. Use this screen to populate your Access List to permit or block certain MAC address access to your wireless network.
- *Advanced Wireless Settings*. Use this screen to configure the Access Point's more advanced wireless settings (e.g. Wireless Isolation, Output Power, etc.).

AP Mode

Use this screen to configure the Access Point operation mode with WDS (Wireless Distribution System).

Administration

You will use the Administration tabs to manage the Access Point.

- *Management*. This screen allows you to customize the password and Simple Network Management Protocol (SNMP) settings.
- *Log*. Configure the Log settings for the Access Point on this screen.
- *Factory Default*. Use this screen to reset the Access Point to its factory default settings.
- *Firmware Upgrade*. Upgrade the Access Point's firmware on this screen.
- *Reboot*. Use this screen to reboot the Access Point.
- *Config Management*. You can back up the configuration file for the Access Point, as well as save the backup configuration file to the Access Point.

snmp: *the standard network management protocol on the Internet.*

firmware: *the software image that runs on a CPU inside a networking device.*

Status

You will be able to view status information for your local network, wireless networks, and network performance.

- *Local Network*. This screen displays system information, including software & hardware version, MAC address, and IP address on the LAN side of the Access Point.
- *Wireless*. This screen will display current information on the Access Point and its wireless networks.
- *System Performance*. This screen will display current information on the Access Point and its data transmissions.

Chapter 6: Configuring the Wireless-G Access Point with Power Over Ethernet

This chapter is a detailed reference guide for the Web-based Utility. You do not need the Utility to start using your Access Point. The Access Point has been designed to be functional right out of the box with the default settings. However, if you'd like to change your settings, you can use the Utility.

The Setup Tab

The first screen that appears is the *Setup* screen. This allows you to change the Access Point's general settings.

Setup

Enter names for the Access Point. The host name can be used to access the Web Utility through the network if DNS has been set up. The device name is for the benefit of identifying your Access Point after you log in.

Host Name. The host name assigned to the Access Point. This host name will be published to DNS server if the Access Point is configured to acquire the IP address through DHCP. In that case, it is recommended to follow the company policy on the host name assignment. The default name is **Linksys**.

Device Name. You may assign any device name to the Access Point. This name is only used by the Access Point administrator for identification purposes. Unique, memorable names are helpful, especially if you are employing multiple access points on the same network. The default name is **WAP54GP**.

Network Setup

The selections under this heading allow you to configure the Access Point's IP address setting(s).

IP Settings

Select **Static IP Address** (default) if you want to assign a static or fixed IP address to the Access Point. Then complete the following:

- **IP Address**. The IP address must be unique to your network. The default IP address is **192.168.1.245**.
- **Subnet Mask**. The Subnet Mask must be the same as that set on the LAN that your Access Point is connected to. The default is **255.255.255.0**.

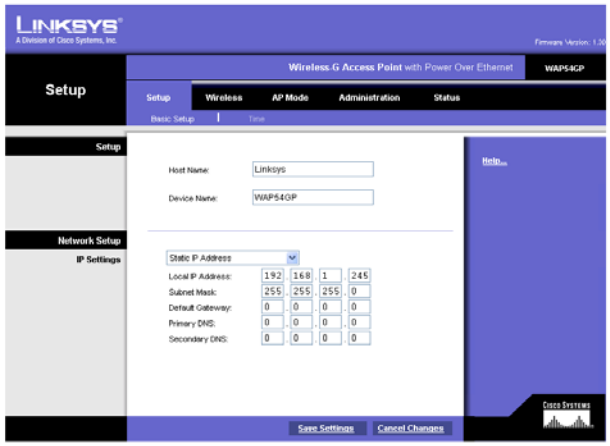


Figure 6-1: Setup - Static IP Address

Select **Automatic Configuration - DHCP** if you have a DHCP server enabled on the LAN that can assign an IP address to the Access Point.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen.

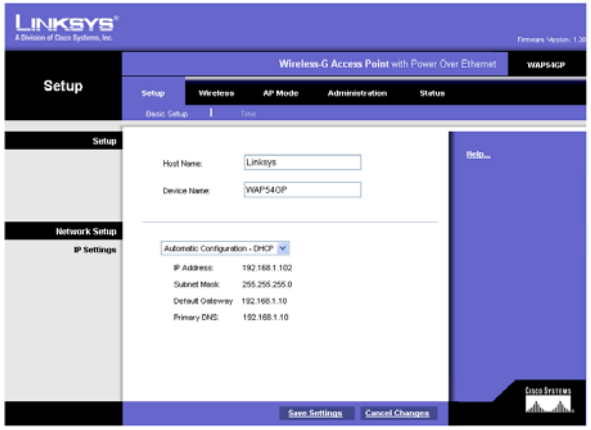


Figure 6-2: Setup - Automatic Configuration - DHCP

The Setup - Time Tab

This allows you to change the Access Point's time settings. The correct time setting can help the administrator search the system log to identify problems.

Time

If the Access Point can access the Web, the time can be set automatically. You can always set the time manually.

Manually. This is the default setting. If it is not already selected, click on Manually. Then use the drop down menus to select the month, day and year. Enter the hour, minute and seconds.

Automatically. When you click on this option, you will need to select your correct time zone from the drop down menu. The time zone is based on GMT (Greenwich Mean Time). After you select the time zone, the Access Point will contact the web-based public time server to get the current time.

Auto Daylight Saving. Enable this option if you want Daylight Saving time to be adjusted automatically according to your time zone. The default is **Disabled**.

User Defined NTP Server. Enable this option if you have set up local NTP server. The default is **Disabled**.

NTP Server IP. If you enabled the User Defined NTP Server, you will need to enter its IP address.

Click **Save Settings** to apply your changes, or click **Cancel Changes** if you don't want to apply the changes. For more intomraion, click **Help** on the righ side of the screen.

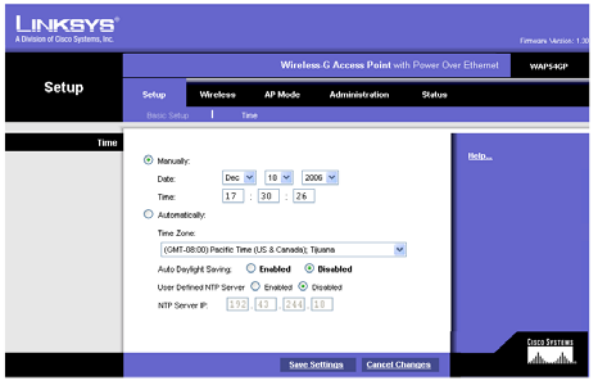


Figure 6-3: Setup - Time

The Wireless - Basic Wireless Settings Tab

Change the basic wireless network settings on this screen. The Access Point can connect to up to eight wireless networks (SSIDs) at the same time, so this screen offers settings for up to eight different SSIDs. All the SSIDs share the same BSSID (MAC address) on this Access Point, so the first one is called Main SSID and others are called Virtual SSIDs.

Figure 6-4: Wireless - Basic Wireless Settings

Wireless Network

Configure the Wireless Network attributes for each SSID.

Wireless Network Mode. Select **Mixed** to allow both Wireless-G and Wireless-B client devices on the network. With this setting the maximum throughput will be reduced. Select **G-Only** for maximum throughput with Wireless-G client devices only. The final selection, **B-Only**, allows only Wireless-B client devices on the network. You can also disable wireless connectivity if you select **Disabled**. The default is **Mixed**.

VLAN Trunk. Select **Enabled** if you want to pass 802.1q VLAN tagged traffic between wired LAN and wireless LAN. Your Access Point will map the VLAN tag (wired side) to a different SSID (wireless side) according to the settings you enter on this screen. Select **Disabled** and your Access Point will drop all tagged traffic coming in from the wired LAN. The default is **Disabled**.

Priority. The default is **Disabled**. Select **Enabled** if you want to assign default traffic priorities. This option is automatically enabled when **VLAN Trunk** is enabled.

In the chart that takes up most of this screen, you can set up the names and attributes of your Main and Virtual SSIDs. VLAN ID column is enabled with **VLAN Trunk** option. VLAN Priority column is enabled with **Priority** option.

SSID. You can enter settings for up to eight wireless networks (SSIDs).

SSID Name. The SSID is the unique name shared among all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure this setting is the same for all devices in your wireless network.

VLAN ID. Select a number between 1 and 4094 to identify this VLAN. Multiple SSIDs can share the same VLAN value.

VLAN Priority. You can assign the priority (802.1p COS bits) for packets coming in from each wireless network by selecting a number from the drop-down menu. The higher the number, the higher the priority will be. The default is 0.

Tx Rate Limiting. You can limit the maximum data rate used in your network to save bandwidth and power consumption on client devices. The actual data rate is determined by an Auto-Fallback mechanism between your Access Point and a client device. The default is **54 Mbps** Mixed or G-Only mode, **11 Mbps** for B-Only mode.

Wireless SSID Broadcast. The default is **Enabled**. This option allows the primary SSID to be broadcast on your network. You may want to leave this function enabled while configuring your network, but make sure that you disable it when you are finished. When enabled, someone could easily obtain SSID information with site survey software and gain unauthorized access to your network.

Click **Enabled** to broadcast the primary SSID to all wireless devices in range. Click **Disabled** to increase network security and prevent the primary SSID from being seen on networked PCs.

Access Point VLAN ID. When **VLAN Trunk** is enabled, enter an ID so that client devices on that VLAN will have access to the Access Point's Web-based Utility. The default is to deny access from any VLAN.

Default VLAN ID. When the **VLAN Trunk** is enabled, this option can be used to set the default VLAN number. This option allows compatibility with the connecting switches.

VLAN Tag. This option can set the default 802.1q VLAN to be tagged or untagged. The default value is tagged. This option is used to be compatible with the connecting switches. Cisco switches usually have default VLAN number 1 and are untagged.

Wireless Channel. Select the appropriate channel to be used among your Access Point and client devices. The default is channel 6. You can also select **Auto** so that your Access Point will select the channel with the lowest amount of wireless interference while the system is powering up. Auto channel selection will start when you click the **Save Settings** button. It will take several seconds to reboot and scan through all the channels to find the best channel. The selected channel will be displayed as **current channel** on the right side.

Click **Save Settings** to apply your changes, or click **Cancel Changes** if you do not want to apply the changes. **Help** information is displayed on the right side of the screen. Click **More** for additional details.

The Wireless - Wireless Security Tab

Change the Access Point's wireless security settings on this screen.

Wireless Security

Enter the security settings for each SSID of the Access Point.

Select SSID. Select the SSID whose security settings you want to configure.

Security Mode. Select the wireless security mode you want to use, **WPA-Personal**, **WPA2-Personal**, **WPA2-Personal Mixed**, **WPA-Enterprise**, **WPA2-Enterprise, WPA2-Enterprise Mixed, RADIUS**, or **WEP**. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption and forward compatible with 802.11e. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) Refer to the appropriate instructions below after you select the Authentication Type and SSID Interoperability settings. For detailed instructions on configuring wireless security for the Access Point, refer to "Appendix B: Wireless Security." To disable wireless security completely, select **Disable**. The default is **Disabled**.

Wireless Isolation (within SSID). When disabled, wireless PCs that are associated to the same Network Name (SSID), can see and transfer files between each other. When **Enabled**, Wireless PCs will not be able to see each other. This feature is very useful when setting up a wireless hotspot location. The default is **Disabled**.

Detailed options for each Security Mode are described below.

Disabled

There is no option to be configured for this mode.

WPA-Personal (aka WPA-PSK)

WPA Algorithms. WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, **TKIP** or **AES**. The default is **TKIP**.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

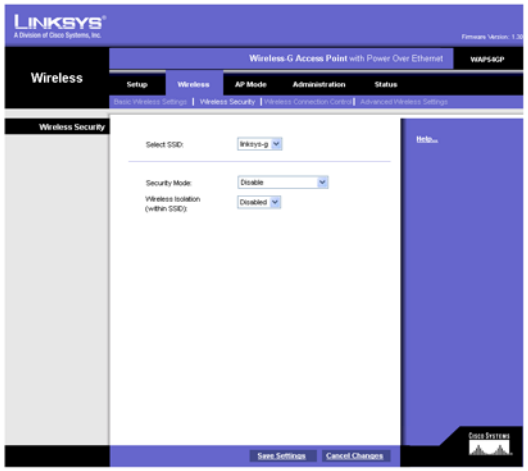


Figure 6-5: Wireless - Wireless Security (Disabled)

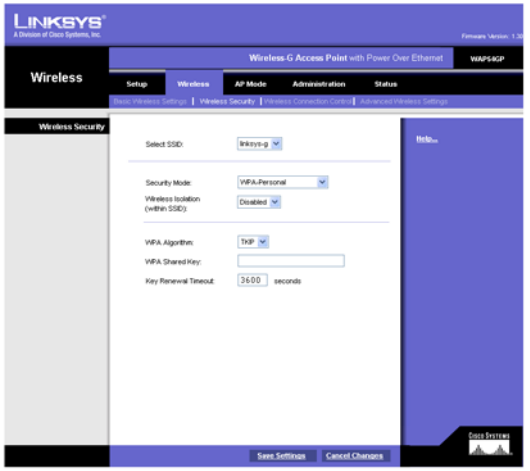


Figure 6-6: Wireless - Wireless Security (WPA-Personal)

WPA2-Personal

WPA Algorithms. WPA2 always uses AES for data encryption.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

WPA2-Personal Mixed

This security mode supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal. The Access Point will automatically choose the encryption algorithm used by each client device.

WPA Algorithms. Mixed Mode automatically chooses TKIP or AES for data encryption.

WPA Shared Key. Enter a WPA Shared Key of 8-63 characters.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

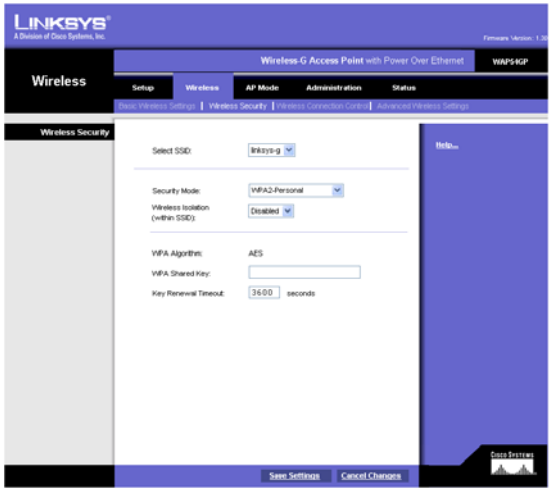


Figure 6-7: Wireless - Wireless Security (WPA2-Personal)

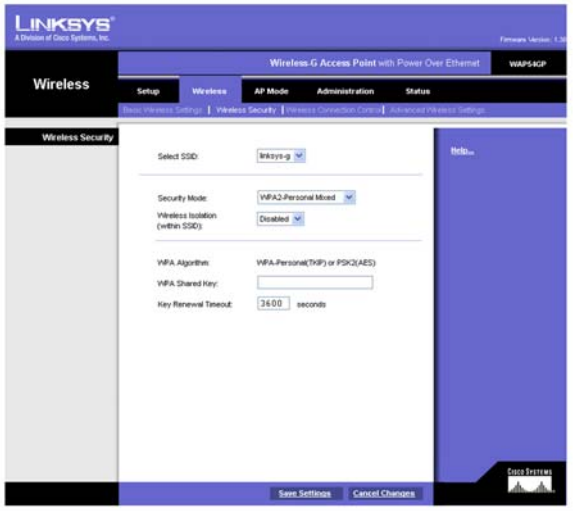


Figure 6-8: Wireless - Wireless Security (WPA2-Personal Mixed)

WPA-Enterprise

This option features WPA used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.)

RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

WPA Algorithms. WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, **TKIP** or **AES**. The default is **TKIP**.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

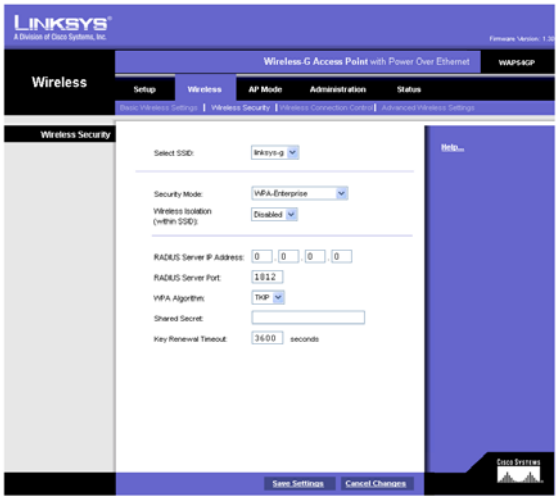


Figure 6-9: Wireless - Wireless Security (WPA-Enterprise)

WPA2-Enterprise

This option features WPA2 used in coordination with a RADIUS server for client authentication. (This should only be used when a RADIUS server is connected to the Access Point.)

RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

WPA Algorithms. WPA2 always uses AES for data encryption.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

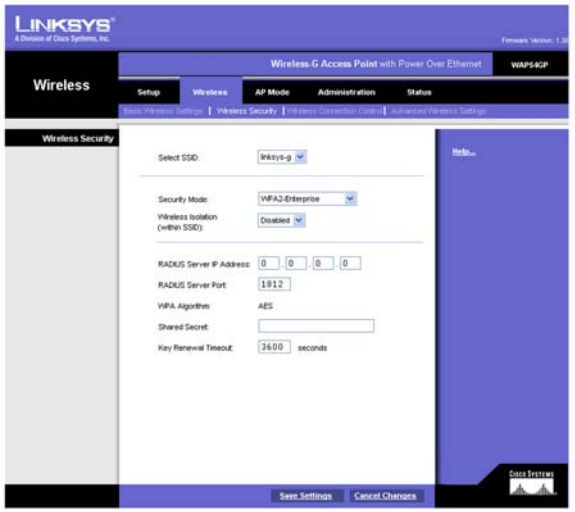


Figure 6-10: Wireless - Wireless Security (WPA2-Enterprise)

WPA2-Enterprise Mixed

This security mode supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise. The Access Point will automatically choose the encryption algorithm used by each client device.

RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

WPA Algorithms. Mixed Mode automatically chooses TKIP or AES for data encryption.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

Key Renewal Timeout. Enter a Key Renewal Timeout period, which instructs the Access Point how often it should change the encryption keys. The default is **3600** seconds.

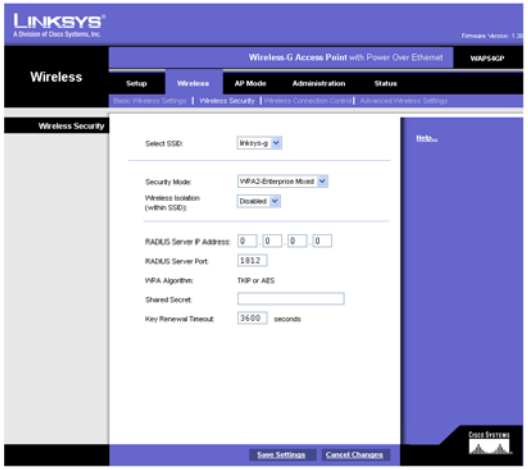


Figure 6-11: Wireless - Wireless Security (WPA2 - Enterprise Mixed)

RADIUS

This security mode is also known as Dynamic WEP with IEEE 802.1X. The RADIUS server is used for client authentication and WEP is used for data encryption. The WEP key is automatically generated by the RADIUS server. A manual WEP key is no longer compatible with Microsoft Windows implementation (due to its weak authentication capability).

RADIUS Server IP Address. Enter the RADIUS server's IP address.

RADIUS Server Port. Enter the port number used by the RADIUS server. The default is 1812.

Shared Secret. Enter the Shared Secret key used by the Access Point and RADIUS server.

WEP

This security mode is defined in the original IEEE 802.11. This mode is not recommended now due to its weak security protection. Users are urged to migrate to WPA or WPA2.

Authentication Type. Choose the 802.11 authentication type as either **Open System** or **Shared Key**. The default is **Open System**.

Default Transmit Key. Select the key to be used for data encryption.

WEP Encryption. Select a level of WEP encryption, **64 bits (10 hex digits)** or **128 bits (26 hex digits)**.

Passphrase. If you want to generate WEP keys using a Passphrase, then enter the Passphrase in the field provided and click the **Generate** key.

Key 1-4. If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** if you do not want to apply the changes. **Help** information is displayed on the right side of the screen.

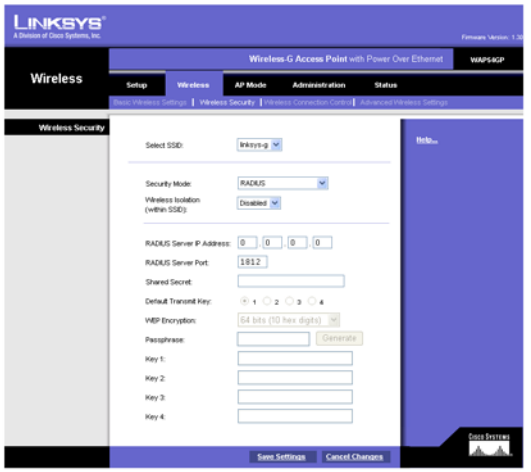


Figure 6-12: Wireless Security - RADIUS

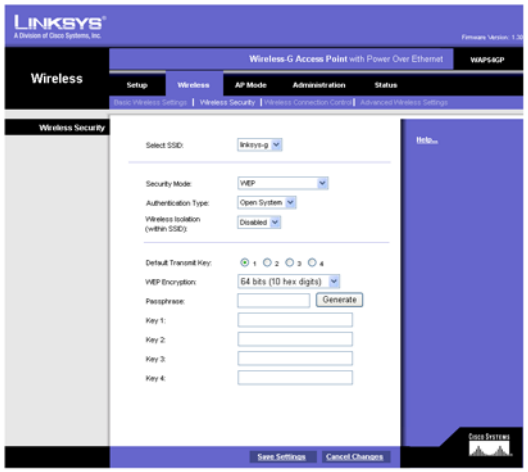


Figure 6-13: Wireless Settings - WEP

The Wireless - Wireless Connection Control Tab

This screen allows you to configure the Connection Control List to control the connection (association) of wireless client devices.

Wireless Connection Control

Connection Control. Choose one of the three options to control the connection (association) of wireless client devices.

- **Disabled**. The default setting.
- **Prevent** MAC Addresses (specific client devices) from connecting to the Access Point.
- **Allow** MAC Addresses (specific client devices) to connect to the Access Point.

Select MAC Address From Networked Computers

Instead of manually entering the MAC address of each client, the Access Point provides a convenient way to select a specific client device from the client association table. Click this button and a window appears to let you select a MAC address from the table. The selected MAC address will be entered into the Connection Control List.

MAC 1-20. Enter the MAC addresses of the wireless devices you want to control.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** if you don't want to apply the changes. Help information is displayed on the right side of the screen.

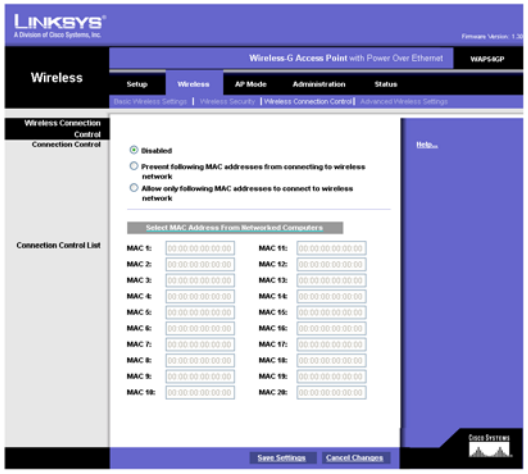


Figure 6-14: Wireless - Wireless Connection Control

Figure 6-1: Select MAC Address from Client Association Table

The Wireless - Advanced Wireless Settings Tab

This screen allows you to configure the advanced settings for the Access Point.

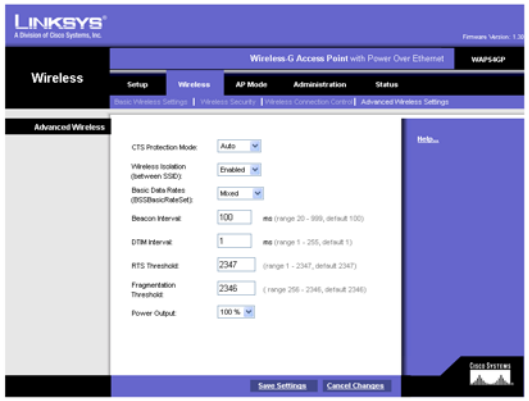


Figure 6-15: Wireless - Advanced Wireless

Advanced Wireless

You can change the data transmission and output power settings for the Access Point.

CTS Protection Mode. CTS (Clear-To-Send) Protection Mode function boosts the Access Point's ability to catch all Wireless-G transmissions but will severely decrease performance. If you keep the default setting **Auto**, the Access Point can use this feature as needed, when the Wireless-G products are not able to transmit to the Access Point in an environment with heavy 802.11b traffic. Select **Disabled** if you want to permanently disable this feature.

Wireless Isolation (between SSIDs). This setting prevents eavesdropping in the network. When it is **Enabled**, wireless frames received on this Access Point will not be forwarded to other wireless networks (SSIDs). For example, if you have a wireless hotspot, you may want to keep the wireless network (SSID) isolated from your other wireless networks (SSIDs).The default is **Enabled**.

Basic Data Rates (BSSBasicRateSet). This setting is a series of rates that are advertised to the other wireless devices as defined in IEEE 802.11 specifications, so they know at which rates the Access Point can support. One of the rates is picked from the list for transmitting control frames, broadcast/multicast frames, or ACK frames. To support both 802.11b & 802.11g devices, use the default **Mixed** mode setting so that frames can be decoded by all devices. To support 802.11g devices only, use the **G-only** mode setting to achieve higher frame rates. For regular data frames, the transmission rate is configured through the Tx Rate Limiting on the Wireless - Basic Wireless Settings tab.

Beacon Interval. This value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Access Point to keep the network synchronized. A beacon includes the wireless networks service area, the Access Point address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

DTIM Interval. This value indicates how often the Access Point sends out a Delivery Traffic Indication Message (DTIM). Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power, but interferes with wireless transmissions.

RTS Threshold. This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2347**. If you encounter inconsistent data flow, only minor modifications are recommended.

Fragmentation Threshold. This specifies the maximum size a data packet can be before splitting and creating a new packet. It should remain at its default setting of 2346. A smaller setting means smaller packets, which creates more packets for each transmission. If you experience high packet error rates, you can decrease this value, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

Power Output. You can adjust the output power of the Access Point to get the appropriate coverage for your wireless network. Select the level you need for your environment. If you are not sure of which setting to choose, then keep the default setting, 100%.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

The AP Mode Tab

On this screen you can change the Access Point's mode of operation. It is also known as WDS (Wireless Distribution System) Mode. You may wish to do this if you want to use the Access Point as a wireless repeater to extend the range of your wireless network. You may also wish to do this if you want to use the Access Point as a wireless bridge; for example, you can use two Access Points in Wireless Bridge mode to connect two wired networks that are in two different buildings.

IMPORTANT: For Wireless Repeater and Wireless Bridge modes, the remote access point must be a second Linksys Wireless-G Access Point with Power Over Ethernet (model number: WAP54GP) or a Linksys Wireless-G Exterior Access Point with Power Over Ethernet (model number: WAP54GPE). The Access Point will not communicate with any other kind of remote access point.

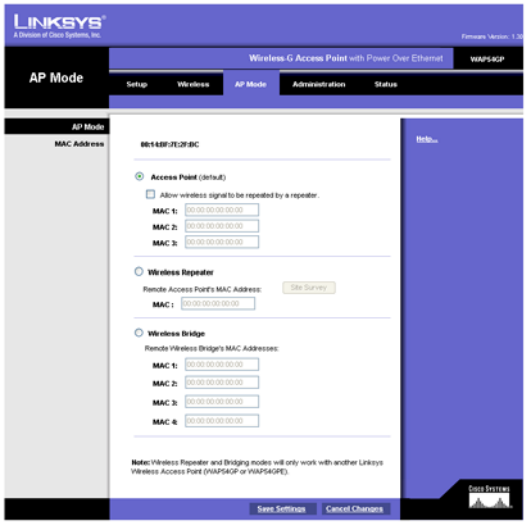


Figure 6-16: AP Mode

AP Mode

The Access Point offers three modes of operation: Access Point, Wireless Repeater, and Wireless Bridge. Some other Access Points distinguish point-to-point bridge mode from point-to-multipoint bridge mode, but this Access Point supports both on the same Wireless Bridge setup. For the Repeater and Bridge modes, make sure the SSID, channel, and security settings are the same for the other wireless access points/devices.

MAC Address

The MAC address of the Access Point is displayed here. This is for the convenience to connect multiple Access Point together through repeater or bridge mode.

Access Point

The Mode is set to **Access Point** by default. This connects your wireless PCs to a wired network. In most cases, no change is necessary. If you want to let the Access Point's signal be repeated, then click the checkbox next to *Allow wireless signal to be repeated by a repeater.* The Access Point can allow the signal to be repeated up to 3 repeaters.

For an example of a repeater, you can use the Access Point with the Linksys Wireless-G Range Expander (model number: WRE54G).

Wireless Repeater

When set to Wireless Repeater mode, the Access Point receives the signal from the remote Access Point and retransmits its signal. (This feature only works with the Linksys Wireless-G Exterior Access Point (model number: WAP54GPE) and Wireless-G Interior Access Point (model number: WAP54GP).

To configure a Wireless Repeater environment, click **Wireless Repeater** and enter the MAC addresses of the remote access points in the *MAC* fields. If you do not know an access point's MAC address, click the **Site Survey** button. Select the access points you want to use and click the **Apply** button. Then click the **Close** button to return to the *AP Mode* screen. If you do not see the access point you want, click the **Refresh** button to run another site survey.

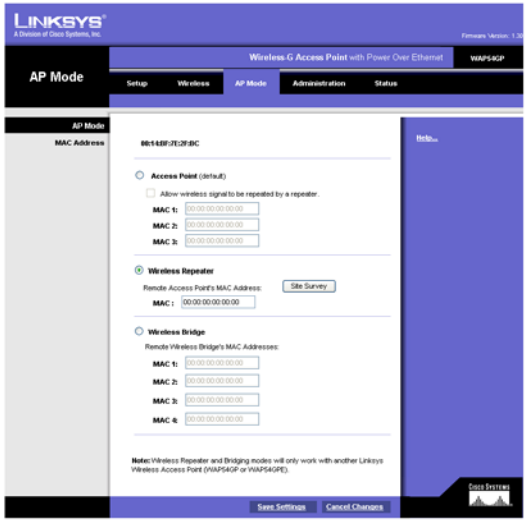


Figure 6-17: Wireless Repeater

Wireless Bridge

This mode connects multiple physically separated wired networks with access points.

If you are trying to create a wireless connection between two wired networks, select **Wireless Bridge** and enter the MAC addresses of the remote wireless bridge/access point in the *MAC 1* fields. If you do not know the remote wireless bridge/access point's MAC address, click the **Site Survey** button. Select the wireless bridge/access point you want to use and click the **Apply** button. Then click the **Close** button to return to the *AP Mode* screen. If you do not see the wireless bridge/access point you want, click the **Refresh** button to run another site survey. The remote wireless bridge/access point also need to be set to Wireless Bridge mode.

If you are trying to create a wireless connection among multiple wired networks, select one Access Point as the hub for point-to-multipoint connection. Enter the MAC address of the remote wireless bridges/access points in the MAC 1-4 fields. The remote wireless bridges/access points will have the Hub's MAC address only in their configuration.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

IMPORTANT: In Wireless Bridge mode, the Access Point can ONLY be accessed by another access point in Wireless Bridge mode. In order for your other wireless devices to access the Access Point, you must reset it to Access Point mode. The two modes are mutually exclusive.

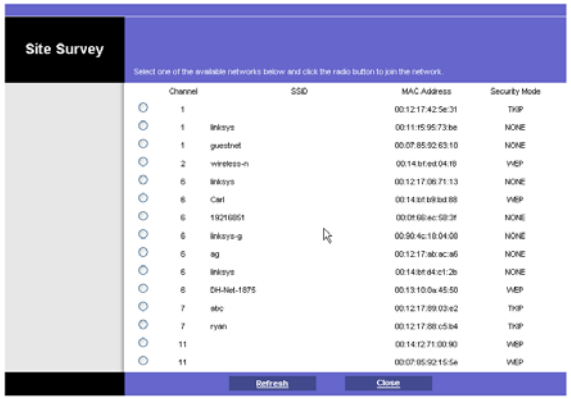


Figure 6-18: Site Survey

The Administration - Management Tab

On this screen you can configure the password, Web Access, and SNMP settings.

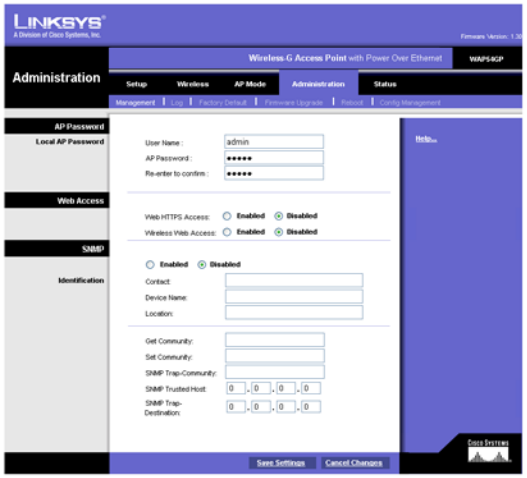


Figure 6-19: Administration - Management

AP Password

You should change the username/password that controls access to the Access Point's Web-based Utility.

Local AP Password

User Name. Modify the administrator username. The default is **admin**.

AP Password. Modify the administrator password for the Access Point's Web-based Utility. The default is **admin**.

Re-enter to confirm. To confirm the new Password, enter it again in this field.

Web Access

To increase the security on accessing Web-based Utility. You can enable HTTPS. Once enabled, users need to use *https://* when accessing the Web-based Utility.

Web HTTPS Access. Use secured HTTP session to access Web based Utility. The default is **Disabled**.

Wireless Web Access. Allow or deny wireless clients to access Web based Utility. The default is **Enabled**.

SNMP

SNMP is a popular network monitoring and management protocol. It provides network administrators with the ability to monitor the status of the Access Point and receive notification of any critical events as they occur on the Access Point.

To enable the SNMP support feature, select **Enabled**. Otherwise, select **Disabled**. The default is **Disabled**.

Identification

Contact. Enter the name of the contact person, such as a network administrator, for the Access Point.

Device Name. Enter the name you wish to give to the Access Point.

Location. Enter the location of the Access Point.

Get Community. Enter the password that allows read-only access to the Access Point's SNMP information. The default is **public**.

Set Community. Enter the password that allows read/write access to the Access Point's SNMP information. The default is **private**.

SNMP Trap-Community. Enter the password required by the remote host computer that will receive trap messages or notices sent by the Access Point.

SNMP Trusted Host. You can restrict access to the Access Point's SNMP information by IP address. Enter the IP address in the field provided. If this field is left blank, then access is permitted from any IP address.

SNMP Trap-Destination. Enter the IP address of the remote host computer that will receive the trap messages.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

The Administration - Log Tab

On this screen you can configure the log settings and alerts of particular events.

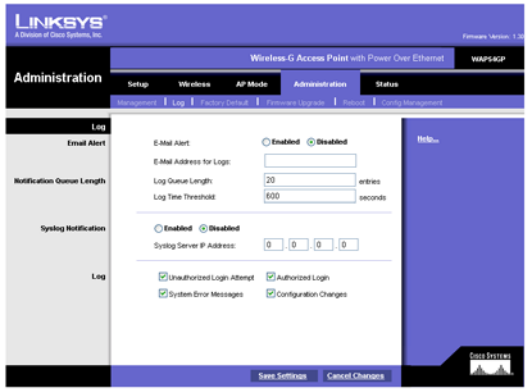


Figure 6-20: The Administration - Log

Log

You can have logs that keep track of the Access Point's activities.

Email Alert

E-Mail Alert. If you want the Access Point to send e-mail alerts in the event of certain attacks, select **Enabled**. The default is **Disabled**.

E-Mail Address for Logs. Enter the e-mail address that will receive logs.

Notification Queue Length

Log Queue Length. You can designate the length of the log that will be e-mailed to you. The default is **20** entries.

Log Time Threshold. You can designate how often the log will be emailed to you. The default is **600** seconds (10 minutes).

Syslog Notification

Syslog is a standard protocol used to capture information about network activity. The Access Point supports this protocol and send its activity logs to an external server. To enable Syslog, select **Enabled**. The default is **Disabled**.

Syslog Server IP Address. Enter the IP address of the Syslog server. In addition to the standard event log, the Access Point can send a detailed log to an external Syslog server. The Access Point's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP server, and number of bytes transferred.

Log

Select the events that you want the Access Point to keep a log.

Unauthorized Login Attempt. If you want to receive alert logs about any unauthorized login attempts, click the checkbox.

Authorized Login. If you want to log authorized logins, click the checkbox.

System Error Messages. If you want to log system error messages, click the checkbox.

Configuration Changes. If you want to log any configuration changes, click the checkbox.

Change these settings as described here and click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Help information is displayed on the right-hand side of the screen, and click **More** for additional details.

The Administration - Factory Default Tab

On this screen you can restore the Access Point's factory default settings.

Factory Default

Note any custom settings before you restore the factory defaults. Once the Access Point is reset, you will have to re-enter all of your configuration settings.

Restore Factory Defaults. To restore the Access Point's factory default settings, click the **Yes** radio button. Then click **Save Settings**. Your Access Point will reboot and come back up with the factory default settings in a few seconds.

Click **Save Settings** to apply your change, or click **Cancel Changes** to cancel your change. Help information is displayed on the right-hand side of the screen.

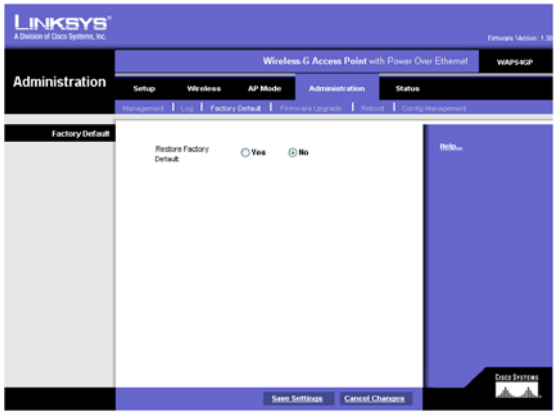


Figure 6-21: Administration - Factory Default

The Administration - Firmware Upgrade Tab

On this screen you can upgrade the Access Point's firmware. Do not upgrade the firmware unless you are experiencing problems with the Access Point or the new firmware has a feature you want to use.

Firmware Upgrade

Before you upgrade the Access Point's firmware, note all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings. To upgrade the Access Point's firmware:

1. Download the firmware upgrade file from the Linksys website, *www.linksys.com*.
2. Extract the firmware upgrade file on your computer.
3. On the *Firmware Upgrade* screen, enter the location of the firmware upgrade file in the field provided, or click the **Browse** button to find the file.
4. Click the **Upgrade** button, and follow the on-screen instructions.

Help information is displayed on the right-hand side of the screen.

Figure 6-22: Administration - Firmware Upgrade

The Administration - Reboot Tab

On this screen you can reboot the Access Point.

Reboot

This feature is useful when you need to remotely reboot the Access Point.

Device Reboot. To reboot the Access Point, click the **Yes** radio button.

Click **Save Settings** to apply your change and the Access Point will reboot itself, or click **Cancel Changes** to cancel your change. **Help** information is displayed on the right-hand side of the screen.

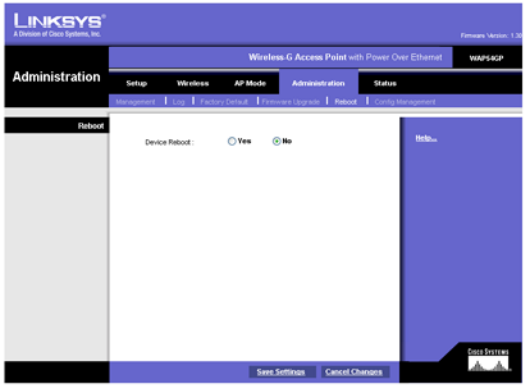


Figure 6-23: Administration - Reboot

The Administration - Config Management Tab

On this screen you can create a backup configuration file or save a configuration file to the Access Point.

Config Management

Use this screen to upload or download configuration files for the Access Point.

Save Configuration. To save a backup configuration file on a computer, click the **Save Configuration to File** button and follow the on-screen instructions.

Restore Configuration. To upload a configuration file to the Access Point, enter the location of the saved configuration file in the field provided, or click the **Browse** button to find the file. Then click the **Load** button.

Help information is displayed on the right side of the screen.

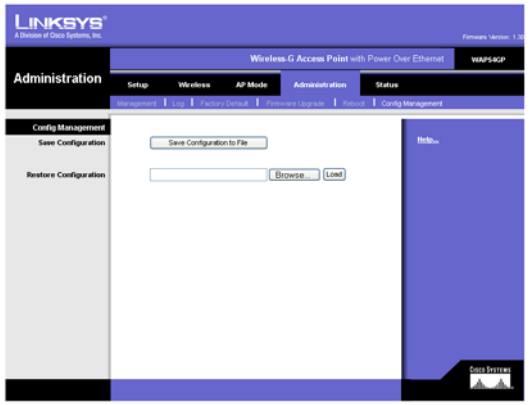


Figure 6-24: Administration - Config Management

The Status - Local Network Tab

The *Local Network* screen displays the Access Point's current status information for the local network.

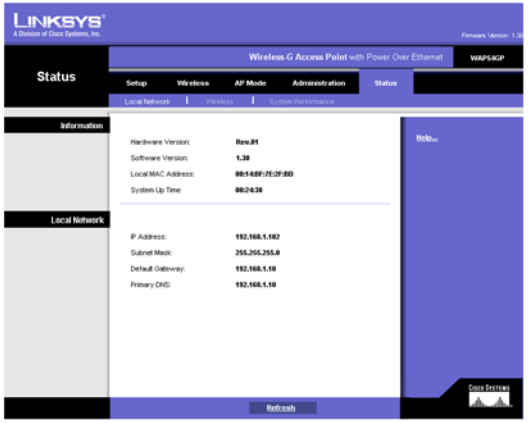


Figure 6-25: Status - Local Network

Information

Hardware Version. This is the version of the Access Point's current hardware.

Software Version. This is the version of the Access Point's current software.

Local MAC Address. The MAC address of the Access Point's Local Area Network (LAN) interface is displayed here.

System Up Time. This is the length of time the Access Point has been running.

Local Network

IP Address. This shows the Access Point's IP Address, as it appears on your local network.

Subnet Mask. This shows the Access Point's Subnet Mask.

To update the status information, click the **Refresh** button. Help information is displayed on the right-hand side of the screen.

The Status - Wireless Tab

The *Wireless* screen displays the Access Point's current status information for the wireless network(s).

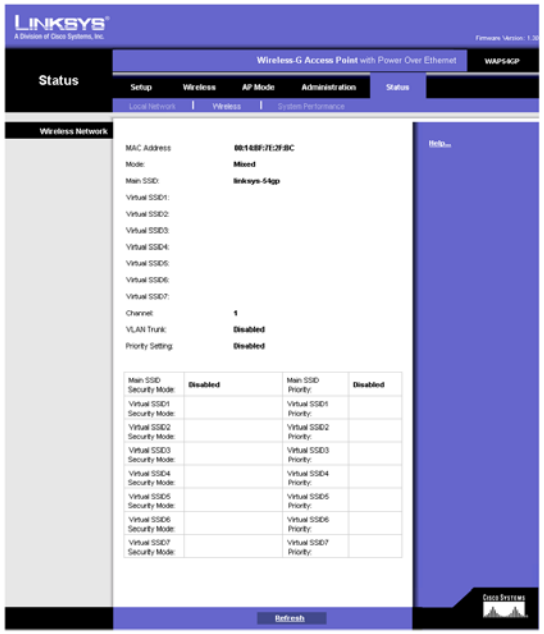


Figure 6-26: Status - Wireless

Wireless Network

MAC Address. The MAC Address of the Access Point's wireless interface is displayed here.

Mode. The Access Point's wireless network mode is displayed here.

Main SSID. The Access Point's primary SSID is displayed here.

Virtual SSID1-7. The Access Point's alternative SSIDs are displayed here.

Channel. The Access Point's Channel setting for the primary SSID is shown here.

VLAN Trunk. This shows if VLAN Trunk is enabled on this Access Point.

Priority. This shows if 802.1p Priority Setting is enabled on this Access Point.

Main SSID & Virtual SSID1-7 Security Mode. This column shows if any type of wireless security (e.g. WEP, WPA-Enterprise, etc.) is enabled for a given SSID.

Main SSID & Virtual SSID1-7 Priority. This column shows 802.1p priority setting for a given SSID. It shows Disabled if *Priority* feature is not enabled.

To update the status information, click the **Refresh** button. Help information is displayed on the right-hand side of the screen.

The Status - System Performance Tab

The *System Performance* screen displays the Access Point's status information for its current settings and data transmissions.

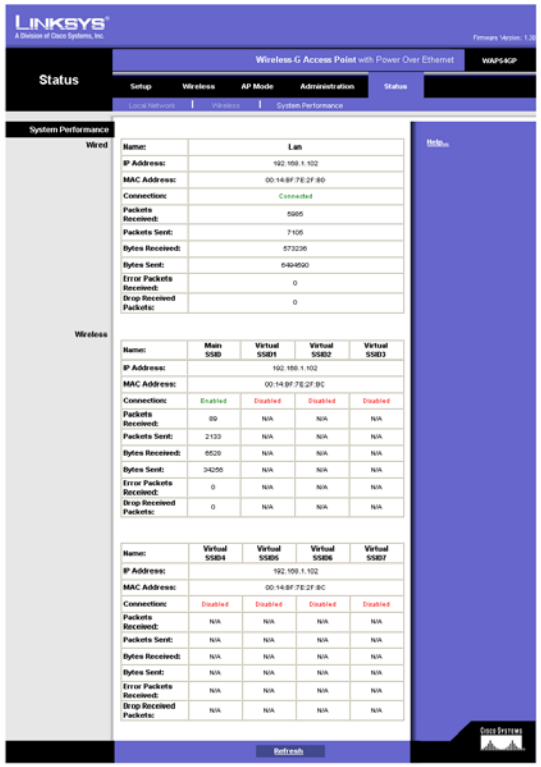


Figure 6-27: Status - System Performance

System Performance

Wired

Name. This indicates that the statistics are for the wired network, the LAN.

IP Address. The Access Point's local IP address is displayed here.

MAC Address. This shows the MAC Address of the Access Point's wired interface.

Connection. This shows the status of the Access Point's connection for the wired network.

Packets Received. This shows the number of packets received.

Packets Sent. This shows the number of packets sent.

Bytes Received. This shows the number of bytes received.

Bytes Sent. This shows the number of bytes sent.

Error Packets Received. This shows the number of error packets received.

Drop Received Packets. This shows the number of packets being dropped after they were received.

Wireless

Name. This indicates the wireless network/SSID to which the statistics refer.

IP Address. The Access Point's local IP address is displayed here.

MAC Address. This shows the MAC Address of the Access Point's wireless interface.

Connection. This shows the status of the Access Point's wireless networks. They are either **Enabled** or **Disabled**.

Packets Received. This shows the number of packets received for each wireless network.

Packets Sent. This shows the number of packets sent for each wireless network.

Bytes Received. This shows the number of bytes received for each wireless network.

Bytes Sent. This shows the number of bytes sent for each wireless network.

Error Packets Received. This shows the number of error packets received for each wireless network.

Drop Received Packets. This shows the number of packets being dropped after they were received.

To update the status information, click the **Refresh** button. **Help** information is displayed on the right-hand side of the screen.

Appendix A: Troubleshooting

This appendix provides solutions to problems that may occur during the installation and operation of the Wireless-G Access Point with Power Over Ethernet. Read the description below to solve your problems. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

Frequently Asked Questions

Can the Access Point act as my DHCP Server?
No. The Access Point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

Can I run an application from a remote computer over the wireless network?
This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Can I play multiplayer games with other users of the wireless network?
Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

What is the IEEE 802.11b standard?
It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

What is the IEEE 802.11g standard?
It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

What IEEE 802.11b features are supported?
The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What IEEE 802.11g features are supported?

The product supports the following IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is Ad-hoc?

An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

What is Infrastructure?

An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

What is roaming?

Roaming is the ability of a portable computer to communicate continuously while its user is moving freely throughout an area greater than that covered by a single Access Point. Before using the roaming function, the user must make sure that the computer is set to the same channel number as the Access Point of the dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and Access Point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data. Achieving these functions simultaneously requires a dynamic RF networking technology that links Access Points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each Access Point and the distance of each Access Point to the wired backbone. Based on that information, the node next selects the right Access Point and registers its address. Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original Access Point or whether it should seek a new one. When a node no longer receives acknowledgment from its original Access Point, it undertakes a new search. Upon finding a new Access Point, it then re-registers, and the communication process continues.

What is the ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is DSSS? What is FHSS? And what are their differences?

Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct Sequence Spread Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers a variety of wireless security methods to enhance security and access control. Users can set it up depending upon their needs.

Can Linksys wireless products support file and printer sharing?

Linksys wireless products perform the same function as LAN products. Therefore, Linksys wireless products can work with NetWare, Windows NT/2000, or other LAN operating systems to support printer or file sharing.

What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802.11 standard.

What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

How do I avoid interference?

Using multiple Access Points on the same channel and in close proximity to one another will generate interference. When employing multiple Access Points, make sure to operate each one on a different channel (frequency).

How do I reset the Access Point?

Press the Reset button on the back of the Access Point for about ten seconds. This will reset the unit to its default settings.

How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between an Access Point and wireless PC will create signal loss. Leaded glass, metal, concrete floors, water, and walls will inhibit the signal and reduce range. Start with your Access Point and your wireless PC in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel. Also, open the Access Point's Web-based Utility. Click the **Wireless** tab and then the **Advanced Wireless** tab. Make sure the Output Power is set to 100%.

Does the Access Point function as a firewall?

No. The Access Point is only a bridge from wired Ethernet to wireless clients.

I have excellent signal strength, but I cannot see my network.

Wireless security, such as WEP or WPA, is probably enabled on the Access Point, but not on your wireless adapter (or vice versa). Verify that the same wireless security settings are being used on all devices in your wireless network.

What is the maximum number of users the Access Point can handle?

No more than 65, but this depends on the volume of data and may be fewer if many users create a large amount of network traffic.

Appendix B: Wireless Security

Linksys wants to make wireless networking as safe and easy for you as possible. The current generation of Linksys products provide several network security features, but they require specific action on your part for implementation. So, keep the following in mind whenever you are setting up or using your wireless network.

Security Precautions

The following is a complete list of security precautions to take (as shown in this User Guide) (at least steps 1 through 5 should be followed):

1. Change the default SSID.
2. Disable SSID Broadcast.
3. Change the default password for the Administrator account.
4. Enable MAC Address Filtering.
5. Change the SSID periodically.
6. Use the highest encryption algorithm possible. Use WPA if it is available. Please note that this may reduce your network performance.
7. Change the WEP encryption keys periodically.

To ensure network security, steps one through five should be followed, at least.

NOTE: Some of these security features are available only through the network router or access point. Refer to the router or access point's documentation for more information.

Security Threats Facing Wireless Networks

Wireless networks are easy to find. Hackers know that in order to join a wireless network, wireless networking products first listen for "beacon messages". These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier). Here are the steps you can take:

Change the administrator's password regularly. With every wireless networking device you use, keep in mind that network settings (SSID, WEP keys, etc.) are stored in its firmware. Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, he, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

SSID. There are several things to keep in mind about the SSID:

1. Disable Broadcast
2. Make it unique
3. Change it often

Most wireless networking devices will give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

Wireless networking products come with a default SSID set by the factory. (The Linksys default SSID is "linksys".) Hackers know these defaults and can check these against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

Change your SSID regularly so that any hackers who have gained access to your wireless network will have to start from the beginning in trying to break in.

MAC Addresses. Enable MAC Address filtering. MAC Address filtering will allow you to provide access to only those wireless nodes with certain MAC Addresses. This makes it harder for a hacker to access your network with a random MAC Address.

WEP Encryption. Wired Equivalent Privacy (WEP) is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

There are several ways that WEP can be maximized:

1. Use the highest level of encryption possible
2. Use "Shared Key" authentication
3. Change your WEP key regularly

WPA. Wi-Fi Protected Access (WPA) is the newest and best available standard in Wi-Fi security. Two modes are available: Pre-Shared Key and RADIUS. Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers, and AES (Advanced Encryption System), which utilizes a symmetric 128-Bit block data encryption. RADIUS (Remote Authentication Dial-In User Service) utilizes a RADIUS server for authentication and the use of dynamic TKIP, AES, or WEP.

IMPORTANT: Always remember that each device in your wireless network MUST use the same encryption method and encryption key or your wireless network will not function properly.

WPA Pre-Shared Key. If you do not have a RADIUS server, select the type of algorithm, TKIP or AES, enter a password in the Pre-Shared key field of 8-64 characters, and enter a Group Key Renewal period time between 0 and 99,999 seconds, which instructs the Router or other device how often it should change the encryption keys.

WPA RADIUS. WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, select the type of WPA algorithm, **TKIP** or **AES**. Enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Last, enter a Group Key Renewal period, which instructs the device how often it should change the encryption keys.

RADIUS. WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router or other device.) First, enter the RADIUS server's IP Address and port number, along with a key shared between the device and the server. Then, select a WEP key and a level of WEP encryption, and either generate a WEP key through the Passphrase or enter the WEP key manually.

Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

These security recommendations should help keep your mind at ease while you are enjoying the most flexible and convenient technology Linksys has to offer.

Appendix C: Upgrading Firmware

The Access Point's firmware is upgraded through the Web-based Utility's Administration - Firmware Upgrade tab. Follow these instructions:

1. Download the firmware upgrade file from the Linksys website, *www.linksys.com*.
2. Extract the firmware upgrade file on your computer.
3. Open the Access Point's Web-based Utility.
4. Click the **Administration** tab.
5. Click the **Upgrade Firmware** tab.
6. On the *Firmware Upgrade* screen, enter the location of the firmware upgrade file in the field provided, or click the **Browse** button to find the file.
7. Click the **Upgrade** button, and follow the on-screen instructions.

Figure C-1: Firmware Upgrade

Appendix D: Windows Help

Almost all wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with the Access Point, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Appendix E: Glossary

This glossary contains some basic networking terms you may come across when using this product. For more advanced terms, see the complete Linksys glossary at http://www.linksys.com/glossary.

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

AES (**A**dvanced **E**ncryption **S**tandard) - An encryption method that supports these key sizes: 128-bit, 192-bit, and 256-bit.

Bandwidth - The transmission capacity of a given device or network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Broadband - An always-on, fast Internet connection.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

Byte - A unit of data that is usually eight bits long

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

Daisy Chain - A method used to connect devices in a series, one after the other.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) - Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**Dem**ilitarized **Z**one) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (**D**omain **N**ame **S**erver) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (**D**igital **S**ubscriber **L**ine) - An always-on broadband connection over traditional phone lines.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (**E**xtensible **A**uthentication **P**rotocol) - A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Firmware - The programming code that runs a networking device.

FTP (**F**ile **T**ransfer **P**rotocol) - A protocol used to transfer files over a TCP/IP network.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) - The communications protocol used to connect to servers on the World Wide Web.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (**I**nternet **P**rotocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (**I**nternet **P**rotocol **Sec**urity) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISP (**I**nternet **S**ervice **P**rovider) - A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address** - The unique address that a manufacturer assigns to each networking device.

Mbps (**M**ega**B**its **P**er **S**econd) - One million bits per second; a unit of measurement for data transmission.

NAT (**N**etwork **A**ddress **T**ranslation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (**P**acket **IN**ternet **G**roper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (**P**ost **O**ffice **P**rotocol **3**) - A standard mail server commonly used on the Internet.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Power **o**ver **E**thernet (**PoE**) - A technology enabling an Ethernet network cable to deliver both data and power.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) - A protocol that uses an authentication server to control network access.

RJ-45 (**R**egistered **J**ack-**45**) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) - The standard e-mail protocol on the Internet.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) - A widely used network monitoring and control protocol.

SPI (**S**tateful **P**acket **I**nspection) **Firewall** - A technology that inspects incoming packets of information before allowing them to enter the network.

SSID (**S**ervice **S**et **ID**entifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) - A set of instructions PCs use to communicate over a network.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) - A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one node to another in a given time period.

TKIP (**T**emporal **K**ey **I**ntegrity **P**rotocol) - a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (**U**niform **R**esource **L**ocator) - The address of a file located on the Internet.

VPN (**V**irtual **P**rivate **N**etwork) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (**W**ide **A**rea **N**etwork)- The Internet.

WEP (**W**ired **E**quivalent **P**rivacy) - A method of encrypting network data transmitted on a wireless network for greater security.

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) - A group of computers and associated devices that communicate with each other wirelessly.

WPA (**W**i-Fi **P**rotected **A**ccess) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix F: Specifications

Model	WAP54GP
Standards	IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af
Ports	Ethernet, Antenna, Power
Buttons	Reset
Cabling Type	UTP CAT 5
LEDs	Power, Ethernet, Wireless-G
Transmit Power	802.11g: 14dBm @ Normal Temp; 802.11b: 18dBm Normal Temp
Security Features	WEP, WPA, RADIUS
WEP Key Bits	64, 128
Dimensions (W x H x D)	1.26" x 7.83" x 6.89" (32 mm x 199 mm x 175 mm)
Unit Weight	1.01 lbs. (0.46 kg)
Power	12V 1A, IEEE802.3af Compliant PoE
Certifications	FCC, CE
Operating Temp.	-4º ~ 140º F (-20º ~ 60º C)
Storage Temp.	-4º ~ 140º F (-20º ~ 60º C)

Operating Humidity	5% to 95% Non-Condensing
Storage Humidity	5% to 95% Non-Condensing

Appendix G: Warranty Information

LIMITED WARRANTY

Linksys warrants to You that, for a period of three years (the "Warranty Period"), your Linksys Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys' entire liability under this warranty will be for Linksys at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by Linksys, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix H: Regulatory Information

FCC Statement

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Safety Notices

Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
Do not use this product near water, for example, in a wet basement or near a swimming pool.
Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Industry Canada (Canada)

This device complies with Canadian ICES-003 and RSS210 rules. Cet appareil est conforme aux normes NMB-003 et RSS210 d'Industrie Canada.

IC Statement

Operation is subject to the following two conditions:

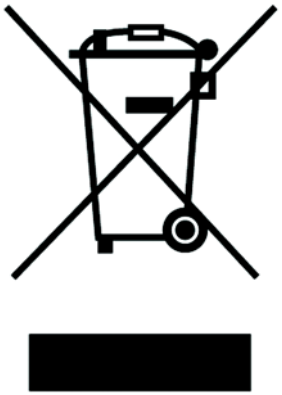
1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Règlement d'Industry Canada

Le fonctionnement est soumis aux conditions suivantes :
1. Ce périphérique ne doit pas causer d'interférences;
2. Ce périphérique doit accepter toutes les interférences reçues, y compris celles qui risquent d'entraîner un fonctionnement indésirable.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:



English

Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Ceština/Czech

Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk/Danish

Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch/German

Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti/Estonian

Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español/Spanish

Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

Ξλληνικά/Greek

Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français/French

Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano/Italian

Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda/Latvian

Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai/Lithuanian

Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir (arba) kurios pakuotė yra pažymėta šiuo simboliu, negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti/Maltese

Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniċipali li ma ġiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-ħanut minn fejn xtrajt il-prodott.

Magyar/Hungarian

Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektől elkülönített eljárást kell alkalmazni. Az Ön felelőssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtőredszereken keresztül számolja fel. A megfelelő hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelőzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands/Dutch

Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk/Norwegian

Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski/Polish

Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português/Portuguese

Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através dos instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Slovenčina/Slovak

Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina/Slovene

Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi/Finnish

Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska/Swedish

Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

For more information, visit www.linksys.com.

Appendix I: Contact Information

Need to contact Linksys? Visit us online for information on the latest products and updates to your existing products at:	http://www.linksys.com or ftp.linksys.com
Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:	800-546-5797 (LINKSYS)
Or fax your request in to:	949-823-3002
If you experience problems with any Linksys product, you can call us at:	800-326-7114
Don't wish to call? You can e-mail us at:	support@linksys.com
If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at: (Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)	949-823-3000